Incident Handler's Journal

Date: July 23, 2024

Entry #1: Documenting a Cybersecurity Incident

This incident was divided into two phases:

1. Detection and Analysis: The scenario explains how the ransomware incident was first identified. The organization reached out to other entities for technical support in this phase.

2. Containment, Eradication, and Recovery: This phase highlights the actions taken to isolate and address the threat. The company, after shutting down their systems, sought external assistance for recovery.

Tools Used: None

The 5 W's:

- Who: A group of unethical hackers
- What: A ransomware incident targeting the company's systems
- Where: A healthcare organization
- When: Tuesday at 9:00 a.m.
- Why: Hackers gained access via a phishing attack and encrypted critical files to demand a ransom.

Date: July 25, 2024

Entry #2: Analyzing a Packet Capture File

Tools Used: Wireshark was utilized for this task. Wireshark is a graphical network protocol analyzer that enables security professionals to capture and analyze network traffic. This tool is valuable for detecting and investigating malicious activities in network traffic.

Date: July 25, 2024

Entry #3: Capturing Network Traffic

Tools Used: Tcpdump, a command-line network protocol analyzer, was used to capture network traffic. Like Wireshark, tcpdump allows users to capture, filter, and analyze traffic, but it's managed via the command-line interface.

Date: July 27, 2024

Entry #4: Investigating a Suspicious File Hash

Tools Used: VirusTotal was used to analyze the file hash in this activity. VirusTotal helps detect malicious content such as viruses, worms, and trojans by analyzing files and URLs. I used VirusTotal to investigate a suspicious file hash flagged by the system.